UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,	
Plaintiff,	
-against-	**OPINION AND ORDER** 09-CR-525 (DLI)
COURTNEY BECKFORD, *et al.*,	
Defendants.	

DORA L. IRIZARRY, United States District Judge:

The instant action arises out of a multi-defendant indictment alleging that defendants conspired to obtain millions of dollars worth of wireless devices by defrauding AT&T, Inc. ("AT&T"), T-Mobile, USA ("T-Mobile"), and Asurion Protection Services, LLC ("Asurion"). The defendants are charged with conspiracy to commit mail and wire fraud, in violation of 18 U.S.C. §§ 1349, 1341, 1343, and aggravated identity theft, in violation of 18 U.S.C. § 1028(A).

Defendant Malachi Burris moves to suppress evidence obtained pursuant to three court-authorized wiretaps of cellular phones owned by co-defendants. (*See generally* Def. Mot. to Supp., Doc. Entry No. 266.) On July 10, 2008, the Honorable Nicholas G. Garaufis, United States District Judge for the Eastern District of New York, authorized a wiretap for telephone number 347-851-0785, which was associated with a pre-paid mobile telephone used by co-defendant Marsha Motayne.[1] (*See* Motayne Wiretap, Doc. Entry No. 305, Ex. 1.) The government supported its application with an affidavit from Christopher M. Stefanac, a Special

[1] Initially, the government believed that the proper spelling of Ms. Motayne's last name was "Montayne." The government corrected this error in its superseding indictment. Accordingly, the court will refer to Ms. Motayne throughout this opinion by her proper name, regardless of whether the documents in question, such as the wiretap applications and authorization orders, contain the proper spelling.

Agent of the United States Secret Service ("U.S.S.S."). (*See* Stefanac Affidavit, Doc. Entry No. 305, Ex. 1.) The government sought renewal of the Motayne Wiretap on August 14, 2008, which Judge Garaufis granted. (*See* Motayne Renewal Wiretap, Doc. Entry No. 305, Ex. 2.) Special Agent Stefanac submitted an affidavit in support of the Motayne Renewal Wiretap application. (*See* Stefanac Renewal Affidavit, Doc. Entry No. 305, Ex. 2.)

The government then requested what has been labeled a "spin off wiretap" on September 3, 2008, in which it sought, and Judge Garaufis granted, authorization to intercept communications over cellular telephones subscribed to by subject Moshe Beizem (primarily used by his son, co-defendant Gabe Beizem), co-defendant Rawl Davis, co-defendant Sonia Bowen (additionally used by co-defendant Rawl Davis), and co-defendant Courtney Beckford (the "Beckford Telephone"). (*See* Spin Off Wiretap, Doc. Entry No. 305, Ex. 3.) Special Agent Stefanac submitted an affidavit in support of the government's application. (*See* Stefanac Spin Off Affidavit, Doc. Entry No. 305, Ex. 3.)

Defendant Malachi Burris also moves to suppress evidence obtained by the U.S. Immigration and Customs Enforcement ("ICE") pursuant to a search of his luggage at John F. Kennedy International Airport ("JFK") on September 13, 2008. (*Id*.) His brother, co-defendant Samuel Burris, joins in the two suppression motions (*see* Samuel Burris Mot. to Supp., Doc. Entry No. 269). The government opposed defendants' motions in their entirety.[2] (*See generally*

[2] At the time the parties briefed these motions, co-defendant Wayne White joined in both of the suppression motions. Additionally, he moved to sever his trial from that of the four defendants who have not pleaded guilty, and to obtain early discovery. (*See* White Mot. to Supp. and to Join in Motions of Co-Defendants, Doc. Entry No. 274.) The government's opposition papers include their opposition to co-defendant White's motions. (*See* Gov't Opp. pp. 43-47.) White has since pled guilty. As such, his motions are denied as moot.

Gov't Opp., Doc. Entry No. 286.) For the reasons set forth below, the Burris defendants' motions to suppress are denied.[3]

BACKGROUND

For the purposes of this opinion, the following facts are considered undisputed by the parties,[4] and are taken from the Stefanac Affidavits unless otherwise noted.

I. The Wiretaps

In 2007, AT&T determined that fraudulently obtained cellular devices were being shipped to addresses within the Eastern District of New York. In October 2007, the New York Electronic Crimes Task Force ("NYECTF"), of which Special Agent Stefanac is a member, initiated an investigation into the conspiracy. NYECTF determined that the subjects[5] of the investigation had obtained unauthorized access to a customer database maintained by AT&T and had devised a fraud scheme whereby subjects used the customer database to add insurance to customer accounts. [6] (Stef. Aff. ¶ 20.) Co-defendant Motayne would contact AT&T's third-

[3] At a motion hearing and status conference held on November 30, 2011, this court orally denied the Burris defendants' motions to suppress and indicated that this written decision would follow. (*See* Minute Entry, November 30, 2011.) Subsequent to the court's denial of the motions, but before the issuance of this written decision, all defendants, including the Burris defendants, pled guilty. (*See* Doc. Entry No. 355.) Nonetheless, the court issues this Opinion and Order for completeness of the record.

[4] These facts are taken from the Stefanac Affidavits and are assumed to be undisputed only to the extent that the defendants do not dispute them in their pretrial motions. To the extent defendants do dispute certain allegations contained in the Stefanac Affidavits, these are addressed in this Opinion and Order.

[5] In the Stefanac Affidavit for the Motayne Wiretap application, the "subjects" of the investigation include: "Courtney Beckford, Malachi Burris, Rawl Davis, Kevin Easton, Lennox Lambert, Marsha Motayne, Maurice Stewart, Rohan Stewart, and others." (Stef. Aff. ¶ 4.)

[6] The Burris defendants dispute whether the government had sufficient evidence to support this statement, which is addressed below. (*See infra*, Discussion Part I.A.)

party insurance carrier, Asurion, to generate a fraudulent insurance claim and have a new cellular device mailed to an address of her selection. (Stef. Aff. ¶ 20.)

Typically, Asurion shipped the new cellular device via private express mail services including FedEx, DHL, or UPS. Individuals working with Motayne, such as co-defendant Lennox Lambert, approached the delivery drivers and offered them money in exchange for the packages containing the new cellular devices. (Stef. Aff. ¶ 22.) Drivers set the packages aside for Motayne and her associates, but electronically scanned the packages as "delivered" with delivery tracking equipment. (*Id*.) The government was able to confirm the delivery process (cash payments in exchange for packages) through two accomplice delivery drivers who became confidential informants, CI-1 and CI-2. (Stef. Aff. ¶¶ 16-17, 22.)

The confidential informants provided additional details of the conspiracy from the perspective of delivery drivers. For example, Motayne contacted CI-1 on a daily basis, informing CI-1 of the presence of fraudulent packages on CI-1's delivery route. (Stef. Aff. ¶ 23.) CI-1 then received a telephone call from Lambert to arrange a location to exchange the packages. (*Id*.) CI-1 received twenty to thirty dollars per confiscated cellular device and was paid in cash on a weekly basis. (*Id*.) Working in conjunction with CI-1, the NYECTF conducted surveillance of these exchanges on numerous occasions in 2007. (Stef. Aff. ¶ 24.) Immediately after two such exchanges, the NYECTF observed Lambert carrying the packages from CI-1 into Motayne's residence. (Stef. Aff. ¶¶ 25-27.) NYECTF also observed co-defendant Rawl Davis retrieve white envelopes from the mailbox outside of Motayne's residence. (*Id*.) CI-1 also made consensually recorded telephone calls to Motayne and Lambert, during which both defendants made incriminating statements. (Stef. Aff. ¶ 29.)

Finally, in connection with the Motayne Wiretap application, Special Agent Stefanac indicated that, after observing and approaching co-defendant William Perkins, co-defendant Perkins admitted complicity in the fraud scheme and confirmed the details of its operations as previously provided by other confidential informants. (Stef. Aff. ¶ 30.)

The government then sought renewal of the Motayne Wiretap and provided additional details as to the operation of the conspiracy. First, since the inception of the investigation, the conspiritors had obtained unauthorized access to T-Mobile customer accounts and were targeting both AT&T and T-Mobile. (Stef. Renewal Aff. ¶¶ 22, 24.) Second, the conspirators began procuring cellular devices through a second fraudulent method. In addition to filing false insurance claims, the conspirators began using their access to unauthorized customer information to add new telephone lines to existing customer accounts. In particular, Motayne contacted AT&T or T-Mobile pretending to be customers, and requested a change of address on the customer accounts and the addition of new telephone lines. (Stef. Renewal Aff. ¶ 24.) The conspirators then intercepted shipments of cellular devices associated with those new telephone lines through the same methods as they had in the past, *i.e.*, bribing delivery drivers with cash in exchange for the fraudulent packages. (Stef. Renewal Aff. ¶¶ 22, 25.) The affidavit submitted in support of the wiretap application included excerpts of conversations recorded pursuant to the Motayne Wiretap corroborating the scheme. During these conversations, Motayne used confidential customer information and spoke in various accents and dialects to request (successfully and unsuccessfully) the addition of new telephone lines to the customer accounts. (Stef. Renewal Aff. ¶¶ 29-48.)

At the time it filed its Spin Off Wiretap application, the government had secured the services of yet a third delivery driver as a confidential informant, CI-3 (Stef. Spin Off Aff. ¶ 26),

as well as further confirmation of the fraudulent delivery scheme from two additional delivery drivers (Stef. Spin Off Aff. ¶ 35). The investigation also had uncovered information that recently ordered cellular devices were being shipped to addresses directly associated with the subjects of the investigation, suggesting a decreased reliance on delivery drivers. (Stef. Spin Off Aff. ¶ 36.)

Further, AT&T identified Got Wireless, a company owned by co-defendant Gabe Beizem and his father, subject Moshe Beizem, as the location from which AT&T's security had been compromised and unauthorized access to customer account information had been procured. (Stef. Spin Off Aff. ¶ 33.) In fact, through its security technology, AT&T was able to link 617 fraudulent insurance claims and associated product shipments to just one of the breaches of access that it discovered at Got Wireless. (*Id*.) T-Mobile also identified Got Wireless as the source of breaches to its security and of information used to fraudulently procure cellular devices. (Stef. Spin Off Aff. ¶ 34.)

The investigators also determined that the conspiracy had broadened its geographic reach. In August 2008, the NYECTF conducted surveillance of the delivery of a fraudulently obtained package with a Philadelphia, Pennsylvania address. (Stef. Spin Off Aff. ¶ 40.) Once the NYECTF determined that the delivery driver had exchanged the package in the same manner as the other drivers, the investigators approached the driver. (*Id*.) The driver indicated that he had given the packages to an individual known as "G" and that he had been doing so for several weeks. (*Id*.) The driver provided NYECTF with the telephone number that he used to contact "G." (*Id*.) As set forth in the Stefanac Spin Off Affidavit:

> A review of telephone calls made to and from this telephone number showed several calls to and from Samuel Burris at 640 E. 80th Street, Brooklyn, NY, an address associated with MALACHI

> BURRIS, one of the SUBJECTS of this investigation. We believe that Samuel Burris is an alias of MALACHI BURRIS.[7]

(*Id*.)

Toll analysis indicated that the subjects were in frequent contact with each other during the period before the government sought the Spin Off Wiretap. (Stef. Spin Off Aff. ¶¶ 45-73.) The government also included excerpts of intercepted calls from the Montayne Renewal Wiretap corroborating the involvement of the various suspects in the ongoing conspiracy. (*See, e.g.*, Stef. Spin Off Aff. ¶¶ 74-75.)

II. The Airport Search

On September 10, 2008, U.S.S.S. agents intercepted a call between defendants Malachi Burris and Courtney Beckford on the Beckford Telephone. They discussed transporting five packages to Jamaica on a flight from JFK to Jamaica. U.S.S.S. contacted United States Customs and Border Protection ("CBP") and learned that the Burris defendants and co-defendant Beckford were scheduled to travel to Jamaica on September 13, 2008 from JFK. The government obtained a warrant to search their luggage from the Honorable Cheryl Pollak, United States Magistrate Judge for the Eastern District of New York;[8] however, the government did not execute the search warrant. On September 13, 2008, ICE conducted a search of the luggage pursuant to their border search authority. ICE catalogued and photographed the contents of the luggage, which included, among other things, computer hard-disk drives, cellular telephones, and contact information and email accounts for AT&T customers. Additionally, CBP stopped co-

[7] As discussed below, the Burris defendants assail the government for erring in identifying "Samuel Burris" as an alias for Malachi Burris, instead of as another individual or subject.

[8] The Burris defendants challenge this search warrant only to the extent that it relies upon information obtained from the Beckford Telephone. Thus, the court's analysis is limited to whether evidence obtained pursuant to the warrant should be excluded as fruit of the poisonous tree.

defendant Samuel Burris on the jetway to conduct an outbound examination. CBP discovered that he was carrying $8,500 in cash and sixteen cellular telephones.

DISCUSSION

I. The Wiretaps

A. Probable Cause

Title 18, United States Code, Section 2518 sets forth the requirements the government must meet and the findings that an issuing judge must make to authorize a wiretap. In pertinent part, Section 2518(3) requires that the government establish and the issuing judge find:

> (a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in Section 2516 of this chapter;
>
> (b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;
>
> * * *
>
> (c) there is probable cause for belief that the facilities from which, or the place where, the . . . oral . . . communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

The standard for evaluating whether the government established probable cause with respect to these requirements is the same as that for a search warrant. *See United States v. Fury*, 554 F. 2d 522, 530 (2d Cir. 1977). Accordingly, the government establishes probable cause with respect to the requirements of Section 2518 when the "totality of the circumstances" indicate a probability of criminal activity. *Illinois v. Gates*, 462 U.S. 213, 230-32 (1983). The Supreme Court further elaborated that "after-the-fact scrutiny by courts of an affidavit should not take the

form of *de novo* review," and that the issuing court's "determination of probable cause should be paid great deference by reviewing courts." *Id*. at 236.

1) The Original Stefanac and Stefanac Renewal Affidavits

The Burris defendants contend that the government included numerous statements in the Stefanac Affidavits for which there was no probable cause. First, they contend that, with respect to the Stefanac Affidavit for the Motayne Wiretap, there was no probable cause for the government to assert that (i) the subjects were engaged in mail fraud and other violations, (ii) Malachi Burris was a middle manager in the criminal scheme, (iii) the subjects obtained unauthorized access to AT&T customer account information, and (iv) the criminal scheme consisted of a multi-tiered enterprise. Second, with respect to the Stefanac Renewal Affidavit for the Motayne Renewal Wiretap, the Burris defendants challenge these same assertions for lack of probable cause, contending that no new information provided support for the inclusion of these statements in the Stefanac Renewal Affidavit. (Def. Mot. to Supp. pp. 1-5.)

The court finds the government met its burden and established probable cause for the issuance of the wiretap orders. In each of the Stefanac Affidavits, defendant Malachi Burris was listed as a "SUBJECT" and not a "SUBJECT INTERCEPTEE." Under these circumstances, the government is not required to establish probable cause with respect to his precise involvement. Section 2518 requires the government to establish probable cause that at least one individual "is committing, has committed, or is about to commit a particular offense." 18 U.S.C. § 2518(3)(a). "[N]othing in the statute restricts the government from naming in the affidavit individuals as to whom it may not have probable cause." *United States v. Ambrosio*, 898 F. Supp. 177, 184 (S.D.N.Y. 1995). The government set forth sufficient evidence to establish that there was probable cause to believe that several of the subjects were engaged in mail and wire fraud. The

Stefanac Affidavit contains detailed information of the conspiracy obtained from AT&T, surveillance, and reliable confidential informants. (Stef. Aff. ¶¶ 16-17, 20, 22-27, 29-30.)

The Stefanac Affidavit also establishes that the conspirators obtained unauthorized access to AT&T customer account information. AT&T understood that a breach of its electronic records occurred in 2007, and that a high volume of fraudulently obtained cellular telephones were being shipped to addresses within this District. (Stef. Aff. ¶ 16.) The U.S.S.S. began to unfurl the conspiracy through its surveillance of drivers and use of confidential informants. (*Id*.) AT&T was able to confirm that members of the conspiracy had received packages that were obtained due to the breach of its electronic records. (Stef. Aff. ¶ 30.)

The Stefanac Affidavits established the existence of a multi-tiered conspiracy. The lowest tier consisted of the delivery drivers, who set aside the fraudulently ordered packages in exchange for cash payments. The government provided sufficient evidence of this tier by use of surveillance and accomplice/confidential informants. (Stef. Aff. ¶¶ 22-24; Stef. Renewal Aff. ¶ 25). The middle tier consisted of conspirators who confirmed the routes for drivers and the existence of target packages, arranged for pick-up of packages from the drivers, and provided payments to the drivers. The government provided sufficient evidence of this tier again by use of surveillance and accomplice/confidential informants. (Stef. Aff. ¶¶ 22-29; Stef. Renewal Aff. ¶¶ 23-24, 33-44.) Finally, a management or top tier existed. The government had minimal details of how this tier operated, but the evidence established its existence. (Stef. Renewal Aff. ¶¶ 29-32, 45; Stef. Spin Off Aff. ¶¶ 74-75.) The investigation determined that the conspirators had obtained unauthorized access to customer account information, operated in more than one state, and had placed fraudulent orders for cellular devices on a grand scale (nearly $20 million

dollars of fraudulently obtained cellular devices shipped during the investigation). There was sufficient probable cause for the government to assert the existence of a management tier.

2) The Stefanac Spin-Off Affidavit

Apparently defendants contend that there was insufficient evidence to find probable cause to intercept calls to and from the Beckford Telephone. This contention ignores the cumulative evidence contained in the Stefanac Affidavits. Beckford is listed as a "SUBJECT" in each of the applications. (Stef. Aff. ¶¶ 4, 11; Stef. Renewal Aff. ¶ 6; Stef. Spin Off Aff. ¶ 6.) In the application for the Motayne Renewal Wiretap, Special Agent Stefanac indicated that investigators observed Beckford transporting packages containing fraudulently obtained cellular devices to Motayne's residence. (Stef. Renewal Aff. ¶ 14.) On July 25, 2008, the Honorable Steven M. Gold, United States Magistrate Judge for this District authorized the installation and use of a pen register and trap-and-trace on the Beckford Telephone. (Stef. Renewal Aff. ¶ 66.) The government observed similar telephone usage to that of the co-conspirators in that Beckford made a high volume of calls and contacted individuals believed or known to be co-conspirators. Beckford made 216 calls to co-defendant Malachi Burris, as well as twenty-nine calls to co-defendant Ron Shealey, a delivery driver. (Stef. Renewal Aff. ¶ 70.) Finally, CI-3, a delivery driver, indicated that he worked with Beckford to exchange packages fraudulently ordered by the conspirators. (Stef. Renewal Aff. ¶ 77.) Accordingly, the court finds there was sufficient evidence to conclude that probable cause existed that the Beckford Telephone was being used in furtherance of the conspiracy, such that intercepting calls to and from the Beckford Telephone did not run afoul with the Fourth Amendment. *See United States v. Gotti*, 459 F. 3d 296, 343-44 (2d Cir. 2006) (explaining that toll records linking a telephone to a known member of a

conspiracy, in addition to other evidence, satisfied the "totality of the circumstances" standard for probable cause).

B. Alleged False Statements in the Wiretap Applications

Under *Franks v. Delaware*, when "a defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request." *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978). To prevent fishing expeditions, the Court held that, in order to mandate an evidentiary hearing:

> [The challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine. There must be allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof. They should point out specifically the portion of the warrant affidavit that is claimed to be false; and they should be accompanied by a statement of supporting reasons. Affidavits or sworn or otherwise reliable statements of witnesses should be furnished, or their absence satisfactorily explained. Allegations of negligence or innocent mistake are insufficient.

Id. at 171. Further, "if these requirements are met, and if, when material that is the subject of the alleged falsity or reckless disregard is set to one side, there remains sufficient content in the warrant affidavit to support a finding of probable cause, no hearing is required." *Id.* at 171-72. "Probable cause to issue a wiretap order exists when the facts made known to the issuing court are 'sufficient to warrant a prudent man in believing' that evidence of a crime could be obtained through the use of electronic surveillance." *United States v. Ruggiero*, 824 F. Supp. 378, 398 (S.D.N.Y. 1993) (quoting *Beck v. Ohio*, 379 U.S. 89, 91 (1964)). "A reviewing court owes great deference to the prior findings of an issuing judicial officer that probable cause exists." *United*

States v. Salas, 07-CR-577 (JGK), 2008 WL 4840872, *3 (S.D.N.Y. Nov. 5, 2008) (citing *United States v. Wagner*, 989 F. 2d 69, 72 (2d Cir. 1993)).

The Burris defendants assail the government's wiretap applications for violating *Franks* on four grounds. First, they contend that the government's error in identifying Samuel Burris as an alias for Malachi Burris, as set forth in the Stefanac Spin Off Affidavit, amounts to a *Franks* violation. They claim the government intentionally or recklessly included this assertion to establish probable cause to intercept calls to and from the Beckford Telephone. (Def. Mot. to Supp. pp. 8-9.) There is no evidence that the government intentionally or recklessly asserted this erroneous statement. The telephone in question was used at an address associated with defendant Malachi Burris and the informant had no identifying information for the co-conspirator other than that he went by the name "G." Further, even if the government had included the proper information, and named Samuel Burris as a new suspect, that assertion, too, would have supported probable cause. The government repeatedly explained that the conspiracy consisted of a close-knit group of individuals "linked by social, familial, or romantic bonds." (*See, e.g.*, Stefanac Spin Off Aff. ¶ 85.)

Second, they assert that the government inappropriately labeled its application for wiretap authorization for the Beckford Telephone as a "spin-off" from the Motayne Wiretap and that the government labeled it as such to mask the fact that the government had improperly included and relied upon stale information regarding co-defendant Beckford to establish probable cause. (Def. Mot. to Supp. pp. 9-10.) The term "spin-off" has no legal bearing or limitation on what the government may assert in its affidavit. The government was required to and did establish probable cause with respect to each telephone at issue and did not engage in any sort of improper short-cut by labeling the overall application as a "spin off" of the Montayne Wiretap. The

Stefanac Spin Off Affidavit set forth that the investigation intercepted calls on the Montayne Telephone from co-defendants Gabe Beizem and Rawl Davis. (Stef. Spin Off Aff. ¶¶ 46-69, 74-75.) The government did not attempt to hide the fact that the investigation had not intercepted telephone calls to the Montayne Telephone from the Beckford Telephone; rather, the government set forth other reliable proof as to Beckford's involvement. (Stef. Aff. ¶¶ 4, 11; Stef. Renewal Aff. ¶¶ 6, 14, 66, 70, 77; Stef. Spin Off Aff. ¶ 6.)

Further, contrary to the assertions of the Burris defendants, the investigation was ongoing and the government's evidence with respect to Beckford was obtained over the course of many months. Indeed, Magistrate Judge Gold approved the pen register and trap-and-trace request on July 25, 2008, nearly contemporaneous in time with the Motayne and Motayne Renewal Wiretaps, which were sought on July 10, 2009, and August 14, 2008, respectively. It is inaccurate to label the government's evidence as stale or isolated. (Stef. Aff. ¶ 11; Stef. Renewal Aff. ¶¶ 14, 66, 70, 77.)

Nor is there any problem with the government's inadvertent omission to list Beckford as a "SUBJECT INTERCEPTEE." The Burris defendants have made no showing of bad faith by the government. The government established each of the requirements necessary to obtain authorization to intercept calls to and from the Beckford Telephone. There is no Fourth Amendment requirement that the government name each potential interceptee. *See United States v. Donovan*, 429 U.S. 413, 427 n.15 (1977) ("It is not a constitutional requirement that all those likely to be overheard engaging in incriminating conversations be named. Specification of this sort identif(ies) the person whose constitutionally protected area is to be invaded rather than particularly describing the communications, conversations, or discussions to be seized.") (internal quotations and citations omitted).

Third, defendants assert that the government falsely or without probable cause, attributed the role of "middle manager" to defendant Malachi Burris. This contention lacks merit. Defendant Malachi Burris has not submitted an affirmation or any other evidence to dispute his role in the conspiracy. Nor has he made any attempt to explain his failure to do so. As such, he has failed to meet the substantial burden required of a movant under *Franks*.

Fourth, defendants contend that the government's attempt to link an address to both co-defendants Sonia Bowen and Malachi Burris was another reckless or intentional misstatement aimed at falsely establishing probable cause to intercept calls to and from the Beckford Telephone. They claim co-defendants Malachi Burris and Bowen did not share an address at the time the government sought the wiretap authorization and the only record of Bowen living at that address predates the inception of the conspiracy. In support of this argument, the moving papers include an affirmation from Parker Seaborough, a sister of both Burris defendants, and the owner of apartments located at the address in question. (*See* Seaborough Affirm., ¶ 1.)

Nonetheless, this contention lacks merit as the Burris defendants have confused the import of the government's assertions. The government sought to establish the interrelatedness of the conspirators. The government could establish a relationship between co-defendants Bowen and Malachi Burris whether they lived together ten years ago or during the conspiracy. Even if the Seaborough Affirmation is fully credited, it does not negate the fact that these co-defendants could have lived together at some time prior to the inception of the conspiracy, and, at the very least, were acquaintances. Notably, even if this information were eliminated from the affidavit, it would not defeat the court's finding of probable cause as to the Beckford Telephone.

For all the foregoing reasons, defendants have failed to sustain their substantial burden under *Franks* and, thus, the request for a *Franks* hearing is denied.

C. Necessity

An application for wiretap authorization must provide "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous . . . ." and a judge reviewing an application for authorization of a wiretap must make such a finding. This requirement was designed to ensure that "wiretapping is not resorted to in situations where traditional investigative techniques would suffice to expose the crime." *United States v. Kahn*, 415 U.S. 143, 153 n.12 (1974). The Second Circuit has made it clear, however, that "there is no requirement that any particular investigation procedures be exhausted before a wiretap may be authorized." *United States v. Young*, 822 F. 2d 1234, 1237 (2d Cir. 1987) (internal quotation marks omitted).

The Burris defendants contend that there was no need to seek authorization to tap the Beckford Telephone because other, less intrusive investigative techniques were available. It appears that this argument is simply another bite at their probable cause argument, as they argue that the Beckford Telephone was not used after January 2008 and that the Beckford Telephone was not related to the multi-tiered conspiracy. The court addressed these arguments above, as they are similar to the arguments assailing the Stefanac Spin Off Affidavit for failing to establish the requisite probable cause.

To the extent that the Burris defendants attack the application on the ground that the government failed to exhaust alternative investigative techniques, this contention lacks merit. First, the Burris defendants provided nothing more than the conclusory allegation that "[t]here was no need for the wiretap of the Beckford phone." (Def. Mot. to Supp. pp. 11.)

Second, the government set forth in great detail the various alternative investigative techniques that it employed prior to seeking authorization for the Motayne Wiretap and the reasons why the use of such techniques would not assist the government reaching all of its goals. The confidential informants were only useful to uncover the involvement of lower and some middle tier conspirators, *i.e.*, the interactions between Motayne and Lambert with the delivery drivers. Moreover, the government's ability to rely on confidential informants was dramatically reduced by the actions of the subjects. Motayne eventually ceased all contact with CI-1. Further, the subjects shifted from having packages shipped to false addresses (and then set aside by the delivery drivers) to simply having the packages shipped to addresses controlled or associated with the conspirators, thereby eliminating the need for complicit delivery drivers. (Stef. Spin Off Aff. ¶ 36.)

The government was not required to demonstrate that it had exhausted every possible investigative technique before seeking wiretap authorization. Rather, section 2518(3)(c) only requires that the issuing judge be informed of the "nature and progress of the investigation and of the difficulties inherent in the use of normal law enforcement methods." *United States v. Diaz*, 176 F. 3d 52, 111 (2d Cir. 1999) (affirming denial of suppression). The government adequately set forth why the suggested techniques would not work and the information Special Agent Stefanac provided is similar to showings that other courts have found sufficient to satisfy the requirements of 18 U.S.C. § 2518(3)(c). *See United States v. Gruttadauria*, 439 F. Supp. 2d 240, 248 (E.D.N.Y. 2006) (holding that "the order substantially complied with the requirements in 18 U.S.C. § 2518(1)(c)"); *see also Salas*, 2008 WL 4840872, at *5-6 (denying suppression of wiretap evidence as the government sufficiently set forth reasons for the necessity of the wiretap and why alternative measures would fail).

Nor was the government required to rely solely upon surveillance and confidential informants simply because those techniques had succeeded in the past. *See United States v. Hinton*, 543 F. 2d 1002, 1011 (2d Cir. 1976) (explaining that "even though state or federal officers may have garnered sufficient information without the use of wiretaps to support an indictment against [a low level conspirator], and possibly against a few others, there was every reasons to believe that additional co-conspirators were involved who could not be successfully investigated without wiretapping"). In many instances, as in this case, these techniques assist the government in building its case against low level conspirators, but not the leaders. The government's success with respect to using these techniques to gather evidence against low level conspirators should not be used to penalize the government from gathering evidence against the leaders. *Cf. United States v. Hogan*, 122 F. Supp. 2d 358, 361 (E.D.N.Y. 2000) ("The affiant also explained why traditional investigative techniques would not be successful in achieving the goals of the investigation, which were not merely the apprehension of the defendant, but the gathering of evidence beyond a reasonable doubt about his entire narcotics operation, including his suppliers, customers and subordinates.").

D. Unauthorized Interception and the Failure to Minimize

The Burris defendants have no standing to challenge the government's failure to minimize telephone conversations intercepted on the Beckford Telephone. It is well-settled that the "suppression of the product of a Fourth Amendment violation can be successfully urged only by those whose rights were violated by the search itself, not by those who are aggrieved solely by the introduction of damaging evidence." *United States v. Alderman*, 394 U.S. 165, 171-72 (1969) ("Fourth Amendment rights are personal rights which, like some other constitutional rights, may not be vicariously asserted."); *United States v. Gallo*, 863 F. 2d 185, 192 (2d Cir.

1988) (affirming the denial of suppression of evidence obtained from surveillance of a co-defendant's home as admissible against appellants because the appellants had no interest in the alleged Fourth Amendment violations suffered by their co-defendant, and, thus, lacked standing). Further, the Burris defendants do not claim any possessory or proprietary interest in the Beckford Telephone. *See Salas*, 2008 WL 4840872, at *8 (explaining that "only an individual with a privacy interest in the subject telephone, or in the premises in which the telephone is located, has standing to contest the minimization procedures employed by law enforcement agents"). Accordingly, the motion to suppress on the grounds of failure to minimize the Beckford Telephone wiretap is denied.

E. Request for Cell-Site and Subscriber Information

The Burris defendants contend that the government improperly sought cell-site information in each of the wiretap applications. In support of their argument, they cite to a decision from the Honorable Colleen McMahon, United States District Judge for the Southern District of New York, in which she rejected a request from the government to obtain cell-site information. *See in the Matter of an Application of the United States of America for an Order Authorizing the use of a Pen Register with Caller Identification Device Cell Site Location Authority on a Cellular Telephone*, 2009 WL 159187 (S.D.N.Y. Jan. 13, 2009). The request at issue in that case is easily distinguishable from the request the government sought in connection with the Motayne, Renewal, and Spin Off Wiretap applications. In the case before Judge McMahon, the government sought the warrantless authorization of prospective cell-site information in connection with a request for a pen register. The government claimed that its authority to request cell-site information in this manner derived from the interrelatedness of certain provisions found in the Pen Register Statute, 18 U.S.C. § 3121, *et seq.*, the

Communications Assistance for Law Enforcement Act of 1994, 47 U.S.C. § 1001, *et seq.*, and 18 U.S.C. § 2703. *See id*. at *2.

In the case at hand, the government sought prospective cell-site information in connection with applications for authorization of wiretaps of those same cellular telephones for which the government established probable cause. These applications are not an instance in which the government is seeking to obtain cell-site information under a self-proclaimed evidentiary standard that is less than probable cause and one that is the subject of divergent, emerging case law. Here, the government sought cell-site information in connection with a traditional wiretap application. Thus, the authorizations contained in these applications do not run afoul of the cases in which courts have declined to authorize the warrantless release of cell-site information. The cases cited by the Burris defendants are inapposite.

Moreover, it was completely proper for the government to seek subscriber information in its wiretap applications. The government established the requisite probable cause to intercept communications conducted over the various phones. In doing so, the government demonstrated that the identity of the subscribers of those intercepted telephones would be relevant and material to its investigation. *See United States v. Clarke*, 07-CR-776 (ERK)(VVP), 2008 WL 2228991, *8 n.5 (E.D.N.Y. May 28, 2008) ("It is self-evident, of course, that the use of the Phillips Telephone necessarily involved other telephones and communications devices with which the Phillips Telephone was in contact. It is therefore reasonable to believe that records concerning those other telephones and communications devices would be relevant and material to the criminal investigation discussed in great detail, and about which numerous "specific and articulable facts" are disclosed, in the wiretap applications."). Accordingly, the Burris defendants' motions to suppress cell-site and subscriber information are denied.

II. The Airport Search

The Burris defendants attack the search of luggage belonging to them, and co-defendant Beckford on two grounds.[9] First, they contend that, to the extent the court determines that the government lacked probable cause to intercept telephone calls on the Beckford Telephone, the court must exclude evidence obtained from the luggage search as fruit of the poisonous tree. As an initial matter, the Burris defendants lack standing to contest the search of co-defendant Beckford's luggage. (*See* Part I.D. *supra*.) Moreover, as set forth above, the government established probable cause with respect to interception of telephone calls over the Beckford Telephone and the agents had obtained a search warrant. It was not improper for ICE and CPB to conduct searches at the behest of another agency. *See United States v. Boumelhem*, 339 F. 3d 414, 424 (6th 2003) ("Customs may properly exercise its statutory authority at the behest of the FBI."). Accordingly, any evidence derived from that wiretap authorization will not be excluded on Fourth Amendment grounds.

Second, the Burris defendants contend that the government cannot rely on the authority vested in ICE and CBP to conduct routine searches of passengers and their luggage because the searches in question were not routine, but rather, were conducted to assist the U.S.S.S. in its investigation. "It is well established that the government has broad powers to conduct searches at the border even where . . . there is no reasonable suspicion that the prospective entrant has committed a crime." *Tabbaa v. Chertoff*, 509 F. 3d 89, 97 (2d Cir. 2007). "[A] suspicionless search at the border is permissible under the Fourth Amendment so long as it is considered to be 'routine.'" *Id*. at 98 (*citing United States v. Irving*, 452 F. 3d 110, 123 (2d Cir. 2006)). To

[9] Ultimately, this issue became moot as the government eventually represented that it would not seek to introduce this evidence at trial against defendants Beckford, Malachi Burris and Samuel Burris and, as mentioned in footnote 3 above, these defendants pled guilty after jury selection. (*See* Doc. Entry No. 355.)

determine whether a search is routine or not, courts evaluate "the level of intrusion into a person's privacy." *Tabbaa*, 509 F. 3d at 98 (*quoting Irving*, 452 F. 3d at 123)). In the case at hand, ICE searched the defendants' luggage, taking photographs and cataloguing its contents. CPB conducted a pat-down search of defendant Samuel Burris and located $8,500 in cash and sixteen cellular telephones. These actions, taken individually, are well within what is considered routine, and the fact that the CBP and ICE agents had additional probable cause to conduct the searches does not necessarily cross the line into non-routine. *See Tabbaa*, 509 F. 3d at 98-100 (holding that the questioning, fingerprinting, and photographing of individuals entering the United States after attending a cultural event in Canada was routine and did not violate the Fourth Amendment). Accordingly, the Burris defendants' motion to suppress the evidence obtained pursuant to the searches conducted at JFK is denied.

CONCLUSION

For the reasons set forth above, the Burris defendants' motions to suppress are denied.

SO ORDERED.

Dated: Brooklyn, New York
June 1, 2012

/s/
DORA L. IRIZARRY
United States District Judge